DATE(S) ISSUED:

4/12/2011

SUBJECT:

Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (MS11-022)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft PowerPoint, a program used for creating presentations. These vulnerabilities can be exploited by opening a specially crafted PowerPoint file received as an email attachment, or by visiting a web site that is hosting a specially crafted PowerPoint file. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

• Microsoft Office XP

• Microsoft Office 2003

• Microsoft Office 2007

• Microsoft Office 2004 for Mac

• Microsoft Office 2010

• Microsoft PowerPoint Viewer Service

RISK:

Government:

• Large and medium government entities: **High**

• Small government entities: **High**

Businesses:

• Large and medium business entities: **High**

• Small business entities: **High**

Home users: **High**

DESCRIPTION:

Three vulnerabilities exist due to the way that Microsoft PowerPoint reads an invalid record in a specially crafted PowerPoint file. As a result, an error is generated and memory is corrupted. These vulnerabilities can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted PowerPoint presentation as an email attachment. In the Web based scenario, a user would visit a website and then open the specially crafted PowerPoint presentation that is hosted on the page.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

• Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

• Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

• Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.

• Remind users not to open email attachments from unknown or untrusted sources.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/bulletin/ms11-022.mspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0655

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0656

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0976

Security Focus:

http://www.securityfocus.com/bid/46228

http://www.securityfocus.com/bid/46228http://www.securityfocus.com/bid/47251
http://www.securityfocus.com/bid/47252